DERWENT-ACC-NO: 2002-492508

DERWENT-WEEK: 200253

TITLE: Method for securing financial calls made through mobile telephones, comprises use of mother and diversified keys located at mobile telephone and server and accessed by personal identification number

INVENTOR: CREGO, P

PATENT-ASSIGNEE: MERCURY TECHNOLOGIES SARL[MERCN]

PRIORITY-DATA: 2000FR-0014825 (November 17, 2000)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
FR 2817107 A1	May 24, 2002	N/A	009	H04Q 007/32

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO	APPL-DATE
FR 2817107A1	N/A	2000FR-0014825	November 17, 2000

INT-CL (IPC): G06F017/60, H04M001/66 , H04Q007/32

ABSTRACTED-PUB-NO: FR 2817107A

BASIC-ABSTRACT:

NOVELTY - A WAP server (3) receives a user request and asks a library (4) for a certificate request which is sent to the user mobile (2). An applet in the user SIM card asks for the user identification and if correct unlocks access to a cryptographic key, calculates a dynamic certificate which depends on the message and key and sends it to the server which makes the service available if the certificate is valid

USE - To make financial calls over mobile telephones secure. Particular application to Banking and Stock Exchange transactions

ADVANTAGE - The method is adapted to mobile telephony and does not

require a
dedicated infrastructure such as PC with card reader

DESCRIPTION OF DRAWING(S) - The drawing shows the method of making mobile calls
secure.(The drawing includes non-English language text)

User mobile 2

WAP server 3

Certification library 4

CHOSEN-DRAWING: Dwg.1/1

TITLE-TERMS: METHOD SECURE FINANCIAL CALL MADE THROUGH MOBILE TELEPHONE
COMPRISE MOTHER DIVERSE KEY LOCATE MOBILE TELEPHONE SERVE ACCESS
PERSON IDENTIFY NUMBER

DERWENT-CLASS: T01 T05 W01 W02

EPI-CODES: T01-N01A1; T01-N02A2; T05-L02; W01-A05A; W01-A05B; W01-B05A1A;
W01-C05B3C; W01-C05B4E; W02-C03C1A;

SECONDARY-ACC-NO:
Non-CPI Secondary Accession Numbers: N2002-389385

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 817 107**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **00 14825**

(51) Int Cl[7] : **H 04 Q 7/32**, H 04 M 1/66, G 06 F 17/60

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 17.11.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 24.05.02 Bulletin 02/21.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *MERCURY TECHNOLOGIES SARL Société à responsabilité limitée* — FR.

(72) **Inventeur(s) :** CREGO PIERRE.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :**

(54) SIGNATURE ELECTRONIQUE SUR LE RESEAU GSM/GPRS ET UMTS.

(57) La demande concerne un procédé de signature électronique et les applications de ce procédé.

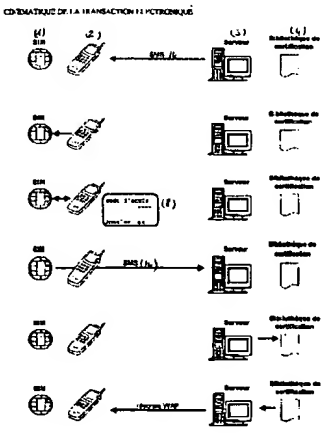
Le procédé de signature électronique selon l'invention met en oeuvre des réseaux de téléphonie mobile (13) de type GSM / GPRS et UMTS. On calcule des signatures à la volée, lors d'une session voix ou données, en utilisant, via un canal de signalisation (14) notamment un canal SMS, au moins une clé mère (11) et des clés diversifiées issues de ladite clé mère (12).

Ladite clé mère et lesdites clés diversifiés sont respectivement enregistrées:

. dans une zone mémoire (9) d'un serveur protégé (3) et

. dans une zone mémoire (9) de la carte SIM (1) d'un téléphone mobile (2).

L'accès à ladite zone mémoire de la carte SIM étant contrôlé par un code d'identification personnel (8).



FR 2 817 107 - A1

Signature électronique sur le réseau GSM/GPRS et UMTS.

1) Domaine technique d'intervention

Cette demande de brevet se situe dans les transactions sécurisées et notamment dans le champ d'application de la monétique. Elle concerne les applications de signature électronique à travers un terminal mobile de nature GSM ou de personnel assistant si celui-ci comporte un lecteur de carte à puce.

1 Exposé du problème

A ce jour il est parfaitement possible d'authentifier une personne à travers sa carte à puce, des jetons sécurisés, de l'empreinte vocale ou digitale mais cela suppose des infrastructures transactionnelles dédiées ou de nature bancaire (PC avec lecteur carte à puce, terminal de paiement..). Ceci demande un investissement particulier.

L'objectif du concept est d'offrir une authentification de type grand public à travers les mobiles GSM existants, en utilisant la carte SIM intégrée au terminal. Plus de la moitié du Commerce Electronique dans les années passera par les terminaux mobiles. A ce jour, il n'existe pas de solution simple offrant une authentification forte de l'utilisateur. Bien que la carte SIM soit identifiée par l'opérateur télécommunications à chaque communication, cela ne suffit pas en terme de sécurité à entrer dans les nouveaux services offerts par l'Internet Mobile.

Le concept de sécurité transactionnelle s'établi entre deux points, d'un côté une machine logicielle intégrée à la carte SIM permet de faire des authentifications à la volée sur plusieurs prestataires de services et de l'autre un serveur de reconnaissance, calcule et compare les signatures reçues.

La carte SIM intègre différentes applications avec des niveaux de sécurité adaptés à chaque service.

L'originalité de cette opération est qu'une carte à puce peut calculer des signatures électroniques à la volée suivant des clés de longueur variable et cohabitant sur la même carte.

Les services possibles :

- Accès sécurisé à un bouquet de services WAP (banques à distance, ordres de bourses, réservations, applications billettiques etc...)
- Accès sécurisé à un service vocal (messageries, e-mail, text to speech)
- Rechargement de cartes prépayées pour des services opérateurs,
- Applications B to B, B to C, B to E....
- Accès sécurisé sur un portail de services entreprise (site WEB)
- Paiements privatifs
- Applications Ventes à Distance

L'application répond au besoin par l'intégration au sein du téléphone mobile, d'une solution sécuritaire souple, indépendante de l'application protégée, et **supportant la sécurisation simultanée de multiples applications** en assurant néanmoins **leurs étanchéités**.

Elle permet l'authentification forte du client, c'est à dire la certitude que l'abonné qui accède au service est un **abonné authentique, autorisé à effectuer cet accès**.

A notre connaissance, il n'existe pas de services utilisant ces concepts sur le marché.

2 Description d'une application

Eléments constitutifs de l'offre

L'offre produit se compose

1. d'un logiciel (**applets**), adaptée à toutes les versions de carte SIM actives du marché
2. d'une **bibliothèque de certification** utilisée par un serveur permettant le dialogue par SMS avec l'applet.

Il permet :

- le calcul sur le téléphone mobile de certificats dynamiques (utilisables une seule fois, donc non re jouables), après saisie par l'usager un code porteur applicatif,
- la modification des clés par des fonctions disponibles sur le mobile (fonction Over The Air)
- la modification par l'usager de son code porteur application.

3 Synoptique d'une authentification

3.1 *Analyse de l'authentification*

Références numériques :

- Carte SIM =1
- Terminal Mobile ou poste client =2
- Serveur d'information de nature WAP ou autre =3
- Bibliothèque de certification =4
- Applets sur carte SIM=5
- Usager ou client final=6
- Application=7
- Code personnel=8
- Zone mémoire du serveur de contrôle = 9
- Zone mémoire de la carte SIM=10
- Clé mère =11
- Clé diversifiée= 12
- Réseau de téléphonie mobile GSM/GPRS/UMTS= 13
- Canal de signalisation SMS ou données =14

Imaginons qu'un service mobile de nature WAP (Wireless Application Protocol) ou autre soit protégé par notre système.

L'usager (6) commence à consulter les pages publiques du service et demande à accéder à la partie du site protégée. Le serveur d'information WAP (3) détecte cette requête et met en route la procédure d'authentification :

1. Il demande à la bibliothèque de certification (4) de calculer un message de demande de certificat à destination du poste client (2) ayant effecteur la requête à une zone sécurisée.

2. Il (3) envoie le message obtenu dans un SMS au mobile GSM (2), et attend une réponse de ce dernier avant de satisfaire à sa requête.

3. Le message est reçu par le mobile GSM (2) et transmis à l'applet présente sur la carte SIM (1)du client, de façon transparente pour l'usager (6).

4. L'applet (5) est réveillée et prend le contrôle du mobile (2). Elle demande la saisie par l'usager (6) du code porteur qui va lui permettre d'accéder au service. L'usager (6) saisit alors son code porteur.

5. Si le code est correct, il déverrouille l'accès à une clé cryptographique au sein de la carte SIM (1). L'applet (5) calcule alors un certificat dynamique dépendant du message reçu et de la clé cryptographique, et renvoie le certificat obtenu dans un SMS à destination du serveur (3).

6. Le serveur (3) reçoit ce message et le fournit à la bibliothèque de certification (4) pour être contrôlé.

7. La bibliothèque (4) indique si le certificat reçu est correct ou non. Le serveur WAP (3) peut ensuite décider de la conduite à adopter : envoi de la page demandée, envoi d'une page d'erreur, etc...

Au total, deux messages SMS ont permis une authentification du client (6) auprès du serveur (3). Le contenu des messages échangés n'apporte pas d'informations à un tiers, et surtout ne permet pas le re-jeu. Le service est donc uniquement délivré aux clients disposant de l'applet (5), et d'une clé, c'est à dire des usagers (6) authentiques .

3.2 Gestion des clés

La gestion des clés est un élément essentiel du système puisqu'elle permet le partage de l'applet entre plusieurs applications, tout en assurant l'étanchéité entre celles-ci.

3.3 Partage du système entre plusieurs applications

L'applet (5) gère jusqu'à 16 clés, identifiées par leur indice (0 à 15). Chaque clé appartient à une application, et chaque application gère un code porteur spécifique, différent du CHV1 demandé lors de la mise sous tension du mobile (2).

Exemple :

Application 1

Code porteur 1

Clé 0

Application 2

Code porteur 2

Clé 3

Clé 4

On peut alors gérer plusieurs applications simultanément comme l'accès à un service de banques à distance (Application 1) et l'accès à un Intranet sécurisé (Application 2). L'usager saisit un code porteur différent selon le service auquel il accède, mais il a toujours la possibilité d'attribuer la même valeur à ses deux codes porteurs.

Une application peut détenir deux clés au sein de la même carte SIM (1): la première pour gérer les certificats actuels, et la seconde en réserve pour de futurs services.

Il est alors possible de faire calculer les certificats avec une autre clé.

Une autre utilisation des clés multiples consiste à gérer plusieurs familles d'utilisateurs d'un même service, ceux qui ont la clé 3 ont par exemple, plus de droits que ceux qui ont la clé 4.

3.4 Modification des clés

Les valeurs des clés de calcul des certificats peuvent être modifiées, grâce à l'usage d'une clé spécifique, unique dans la carte, appelée clé de gestion, et qui n'est utilisée que pour cet usage. Si cette clé est présente sur le serveur (dans la bibliothèque de certification 4), il est alors possible de changer la valeur d'une clé d'indice donné. Cette clé doit donc être détenue par une entité particulière, gestionnaire du système, et garante de son bon fonctionnement.

3.5 Typage des clés

Les clés peuvent être de deux types : simple DES (56 bits) ou triple DES (112 bits). Les premières permettent des calculs plus rapides mais sont plus faibles d'un point de vue cryptographique. L'usage des secondes génère des temps de calculs légèrement supérieurs mais avec une force cryptographique supérieure.

Si les clés de certification peuvent être simple DES, il est recommandé que la clé de gestion soit triple DES.

3.6 Diversification des clés

Tous les usagers d'un même service ont des valeurs de clé différentes. La clé 0 de l'usager A n'est pas la même que la clé 0 de l'usager B. C'est d'ailleurs cette particularité qui permet d'être certain lors du contrôle d'un certificat correct que

l'usager qui l'a renvoyé est bien le bon (si tous les usagers avaient les mêmes clés, ils renverraient tous le même certificat, ce qui permettrait difficilement de les distinguer donc de les authentifier).

Les clés stockées dans les cartes SIM sont des clés diversifiées. Seule la bibliothèque de certification dispose des clés racine d'une application

3.7 Modification des codes

L'usager peut modifier ses codes porteurs par l'interface du mobile, en saisissant l'ancien code, puis le nouveau.

3.8 Evolutivité

Aujourd'hui, l'applet (5) fonctionne sur SMS, seul canal utilisable pour dialoguer avec une applet (5).

Demain, l'usage de protocoles plus rapides (GPRS) déjà prévus par les normes GSM et prochainement intégrées aux mobiles permettront des performances d'authentification bien supérieures, sans rien remettre en cause de l'architecture de sécurité proposée.

3.9 Intégration dans un environnement existant

Le cœur de la sécurité côté serveur est la bibliothèque de certification (4). Développée en C ANSI elle peut être intégrée à n'importe quel environnement.

Elle peut être fournie sous plusieurs formes :

- Fichiers sources intégrables par le client dans son système.
- Adaptation dans un autre environnement logiciel (DLL Windows, API Java, etc...)
- Avec un PC communiquant par un protocole propriétaire sur IP.

Revendications

Procédé de signature électronique mettant en œuvre des réseaux de téléphonie mobile (13) de type GSM / GPRS et UMTS ; ledit procédé étant tel que :

- on calcule des signatures à la volée, lors d'une session voix ou données, en utilisant, via un canal de signalisation (14) notamment un canal SMS ou données, au moins une clé mère (11) et des clés diversifiées issues de ladite clé mère (12) ;

ladite clé mère et lesdites clés diversifiés étant respectivement enregistrées :

- dans une zone mémoire (9)d'un serveur protégé (3) et
- dans une zone mémoire (10) de la carte SIM (1) d'un téléphone mobile (2);

l'accès à ladite zone mémoire de la carte SIM étant contrôlé par un code d'identification personnel (8).

2817107

CINEMATIQUE DE LA TRANSACTION ELECTRONIQUE